An RFID Skimming Gate Using Higher Harmonics

Habraken, René; Dolron, Peter; Poll, Erik; De Ruiter, Joeri

DOI:
10.1007/978-3-319-24837-0_8

An RFID Skimming Gate Using Higher Harmonics

René Habraken[1], Peter Dolron[1], Erik Poll[2], and Joeri de Ruiter[3]

[1] Techno Center, Radboud University Nijmegen
[2] Institute for Computing and Information Sciences, Radboud University Nijmegen
[3] School of Computer Science, University of Birmingham

Abstract. This paper describes a novel antenna design for communicating with ISO/IEC 14443A RFID cards at larger distances than the normal 5-10 cm. The set-up consists of two antennas, one to activate the card at the normal frequency of 13.56 MHz, and another to receive its response at the higher harmonic frequency of 40.68 MHz. The strong field required to power the card at larger distances is likely to drown out its response. By detecting the higher harmonic frequencies originating from the card's response this problem is solved, making communication at larger distances possible. The two antennas, placed 100 cm apart, form an RFID gate that can communicate with cards in the middle of the gate. This is a substantial improvement of the maximum skimming distance of 25 cm reported in literature.

Keywords: RFID, contactless smart card, ISO/IEC 14443, skimming, eavesdropping

1 Introduction

This paper describes a method to extend the communication range with RFID cards, more specifically ISO/IEC 14443 Type A proximity cards [8]. This type is frequently used and it can be found in electronic passports, national ID cards, contactless bank cards and many systems for building access control. It is also compatible with the NFC (Near Field Communication) technology used in mobile phones. The different types of RFID systems operate at different communication distances. For ISO/IEC 14443 the normal operating range is up to 10 centimeters, but most commercially available card readers only achieve a range that is considerably shorter. Increasing the distance at which an RFID card can be activated improves convenience but is a risk for security and privacy.

One of the limiting factors in achieving larger communication distances is the required power for the card. The cards are passive, meaning they have no battery, so they require a strong fluctuating magnetic field for power. But a powerful antenna to active the card at large distances will generate a lot of noise, making it hard to receive the card's response. Here we achieve major improvements by using a resonant coil as a 3rd harmonic antenna to receive

the card's answer. The spectral and physical separation between the activation and reception paths solves the problem that the high power activation antenna drowns out the answer of the card.

The outline of this paper is as follows. Section 2 gives background information on terminology, attack possibilities and the concepts of near field and far field. Section 2 ends with an overview of related work, giving a summary of earlier results with long range antennas. The next three sections describe the antenna designs and experimental results for three scenarios: activating a card at larger distances (Section 3), eavesdropping at larger distances (Section 4), and finally the combination of the two scenarios, communication with a card (activation and reading) at the maximum distance (Section 5). Finally, our conclusions are summarized in Section 6.

2 Background

2.1 Terminology

RFID (Radio Frequency Identification) technology is a wireless communication technique that uses the inductive coupling of coils to transfer data. ISO/IEC 14443 cards require no battery and are powered (and read) at short ranges via electromagnetic (EM) induction. The ISO/IEC 14443 standard distinguishes two types: A and B, which differ in modulation, coding and protocol initialization. This paper only deals with Type A.

Communication with the data carrier, which is called the transponder, card or tag, is started by a reader. Because this reader initiates the protocol, activates the tag, and reads and writes information, it is also called the initiator or transceiver [4]. For reasons of readability it is referred to as reader throughout this paper. Before a tag is activated it must be brought into an alternating electromagnetic field (EM-field) with the right frequency and power level. The distance at which the tag is activated and can receive commands from the reader is called the *activation distance*. The distance at which the reader can still interpret the answer of the tag is the *reply distance* (see Fig. 1). The maximum distance at which a reader can activate a tag *and* receive its response is called the *skimming distance*.

In this paper the communication path from the reader to the tag is referred to as *Reader-to-Tag-link*. The communication path in the other direction is called the *Tag-to-Reader-link*. When these links are established and a complete initialization protocol is executed, it is possible for the reader to communicate with the tag. As the first step of communication the reader will receive and decode the UID (unique ID) of the tag. In our experiments we checked for successful reception of the UID to see if communication was working.

2.2 Attack possibilities

Different attack scenarios on RFID tags can be distinguished.

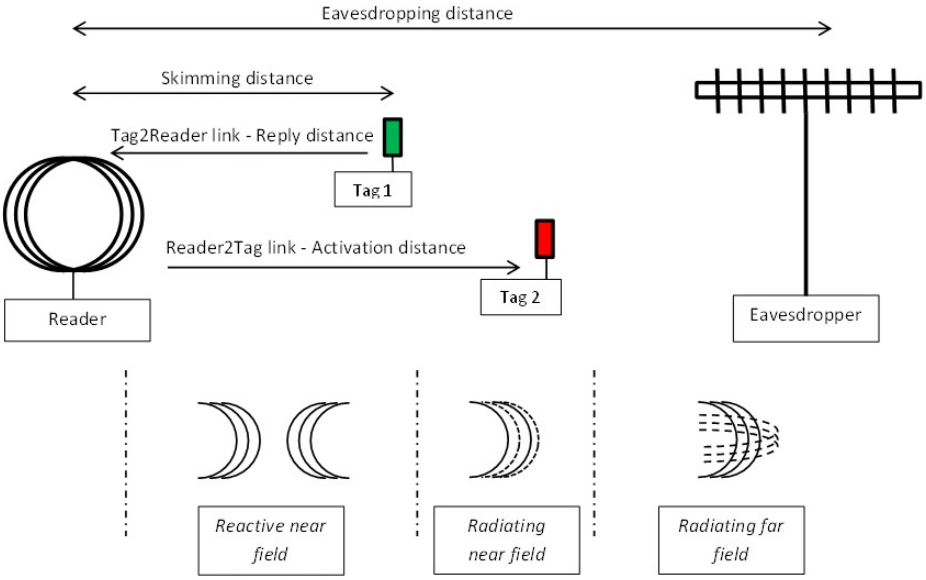

Fig. 1. Terminology

In an **eavesdropping attack**, an attacker intercepts the communication between a tag that is being held close to a normal reader, using a separate eavesdropping antenna. An eavesdropping attack is passive, meaning the eavesdropping antenna that the attacker uses does not have to power the tag, but only listens in on the communication. Because the reader, in contrast to the tag, is an active device and achieves a higher *modulation index* (ratio in signal level between the unmodulated and modulated carrier), the Reader-to-Tag-link is much easier to eavesdrop than the Tag-to-Reader-link.

In a **skimming attack**, an attacker secretly activates a tag and communicates with it. A skimming attack is active, meaning the antenna used has to generate a field to power the tag. This limits the maximum distance for a skimming attack compared to an eavesdropping attack. In a skimming attack a compromise must be made between the activation distance and reply distance. This is because increasing the power of an antenna may increase the activation distance but at the same time decreases the reply distance, as the more powerful and noisy signal from the reader makes it harder to detect the tag's response. We refer to the maximum distance at which a skimming device can communicate with a tag as the *skimming distance*.

NB the term skimming for such an attack can be misleading if one thinks of well-known mag-stripe skimming of bank cards. When skimming mag-stripes, the attacker secretly reads the information on the mag-stripe, and can then make copies to create clones of the original bank card that cannot be distinguished

from the original. For RFID tags, an attacker will not be able to create clones with a skimming attack, as long as the protocol uses some form of challenge-response.

Still, a skimming attack can be used as part of a **relay attack**, where the communication with the tag is relayed to a genuine terminal. If an attacker can for instance relay the communication from a contactless bank card to a payment terminal, this can be considered a digital form of pickpocketing.

2.3 Near and far field

Around an antenna three zones can be distinguished, each with its own properties: the *reactive near field*, *radiating near field* and *radiating far field* (see bottom of Fig. 1). The boundaries between these zones are hard to determine precisely and depend on the surroundings and characteristics of the antenna. Closest to the antenna a varying magnetic field is generated by the changing current through the antenna. This magnetic field, in its turn, also generates a changing electric field [4]. In close proximity of the reader antenna, the magnetic field is predominant over the electric field and this zone is known as the *reactive near field*. Typically this is the area for RFID technology because tags are powered by this magnetic field and communicate via this field. Moving away from the reader the predominant magnetic component drops quickly by the third power of the distance.

A change in voltage on the antenna terminals cannot result in a direct change in the surrounding EM-field and this delay results in the transmission of electromagnetic waves. Being transmitted from the antenna they cannot retroact on the antenna and this marks the end of the reactive near field and the start of the *radiating near field*. For the antennas presented in this paper the border between the reactive and the radiating near field is approximately at 36 cm from the antenna following:

$$D \approx \frac{2L^2}{\lambda} = \frac{2 \times 2^2}{22.11} = 0.36$$

where L is the length of the antenna, D the distance from the antenna and λ the wavelength.

Far field radiation is the most common view on radio waves, e.g. radiation that occurs when broadcasting a radio program or sending a message with a mobile phone. For the *radiating far field* the intensity is inversely proportional to the distance $(1/D)$. The electric and magnetic components, although perpendicular to each other, are in time phase and equal in energy level. The transition to far field radiation marks the unpassable barrier for RFID technology because it is practically impossible to activate a tag. For the ISO/IEC 14443 RFID protocol with a 13.56 MHz carrier frequency the transition from the radiating near field to the radiation far field starts at approximately 3.5 m following:

$$D \approx \frac{\lambda}{2\pi} = \frac{22.11}{6.28} = 3.52$$

For activation and hence skimming we are typically restricted to the reactive near field, whereas eavesdropping is also possible in the radiating far field. But, as will be shown in this paper, it is possible to go beyond the 36 cm with a skimming set-up.

2.4 Related work

Kirschenbaum and Wool [10] built a low cost ($100) antenna that achieved a skimming distance of 25 cm. The antenna is a 40 cm diameter copper tube antenna. The whole set-up is powered by a 12 V battery. They expected that their design could be further improved to achieve a skimming distance of approximately 35 cm.

Hancke [6, 7] describes activation and eavesdropping experiments with different antenna sizes and power usage. The largest activation distance he reports is 27 cm using an A3-sized antenna powered with 4 W. For the maximum eavesdropping distance he reports 400 cm for the Tag-to-Reader-link using a magnetic field antenna. Hancke notes that activating at a tag at a large distance is bad for the possible eavesdropping distance. When he combines activation and eavesdropping (using two antennas) in a skimming attack he uses a smaller activation distance of 15 cm (using an A5-sized antenna and a 4 W amplifier) where he can eavesdrop at 145 cm.

Earlier, Kfir and Wool [9] already predicted skimming distances that could be achieved with various costs and skills, based on experiments and simulations, but without producing a proof-of-concept. Our experiment results are in line with their predictions, as they predict that skimming up to 50 cm should be possible.

The use of higher harmonic frequencies for eavesdropping is not new. Engelhardt et al. [2] demonstrate that eavesdropping on the Tag-to-Reader-link is possible for ISO/IEC 14443 Type A tags at 18 m using the 3^{rd} harmonic. In this scenario a normal reader is used to power the tag. Engelhardt et al. show that a successful detection of the modulation products in the far field relies on the coupling to nearby cables, and that with proper shielding of the cables the harmonics become undetectable.

Carrying out a relay attack not only involves communication with the victims tag, but also interacting with a genuine terminal. Oren et al. [11] looked into extending the range at which one can interact with an ISO/IEC 14443 reader. They reach a 115 cm range with a relay attack, using an active tag to overcome the short range of a passive tag for the Tag-to-Reader-link.

Francis et al. [5] demonstrated that NFC phones can be used to skim tags and then perform relay attacks. Such phones have a short operating range, but have the advantages of being cheap and readily available.

3 Activation at greater distances

3.1 Objective and test set-up

Our first experiments were done on a relatively straightforward skimmer set-up similar to [10] with antenna designs adapted from [12]. Putting two amplifiers in cascade it was possible to power a 50 x 50 cm, transformer-matched, magnetic loop antenna with 60 W. This resulted in a successful skimming distance of approximately 40 cm. The possibility to achieve this distance was already predicted by [9], though we needed a slightly larger and more powerful antenna than predicted. (Kfir and Wool base their prediction on a 40 x 40 cm antenna with the current limited to 4 A). While increasing the amplification, the matching components (necessary to adapt the antenna impedance to a 50 Ω regime for maximum power transfer) heated up to 120° C within two minutes and resulted in a mismatch that eventually broke the antenna and the reader.

By improving the design of the antenna with a gamma matching circuit, it was possible to keep the antenna working over a longer period of time while activating the tag over a long distance. The gamma matching circuit was adapted from [12] and [1] to require the smallest number of high power components compared to other matching strategies (see Fig. 2). We could use this antenna for activation at larger distances, but then the antenna could no longer receive the tag's response. To verify that the tag indeed was activated a pick-up coil was used and held in close proximity to the tag. The signal from this small antenna was fed to the reader to close the communication loop.

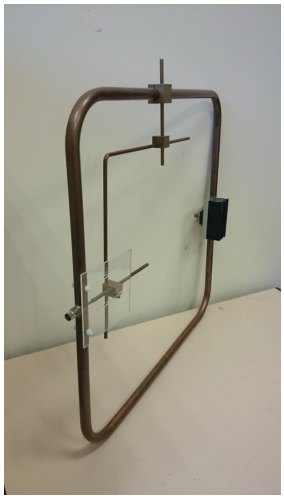

Fig. 2. Gamma-matched antenna

3.2 Results

With the gamma-matched activation antenna and a power of approximately 60 W, an activation distance of 60 cm was reached. The tag's UID was received by the separate pick-up coil and decoded by the reader. Because the same reader was used to power the tag and to decode the answer, the received signal from the tag is in phase with the carrier that was sent by the reader (synchronous detection). Receiving the answer with the pick-up coil was only possible up to a distance of 5 cm from the tag.

4 Eavesdropping using higher harmonics

4.1 Objective and test set-up

The limiting factor when communicating with an RFID tag is not the activation of the tag, but receiving its answer. The tag uses load modulation with a sub-carrier (derived from the carrier frequency) to send its answer to the reader. The limitation of this technique is the ability to alter the strong EM-field generated by the reader by switching on and off a small load on the antenna of the tag. If the field from the antenna is too strong, the influence of tag on this field is too small to be observed by the reader. The effect of the reader on the carrier signal is visible as the dips (modulation index of 100%) on the left side in Fig. 3. The effect of the tag as the smaller dips (and the increase of amplitude) on the right side.

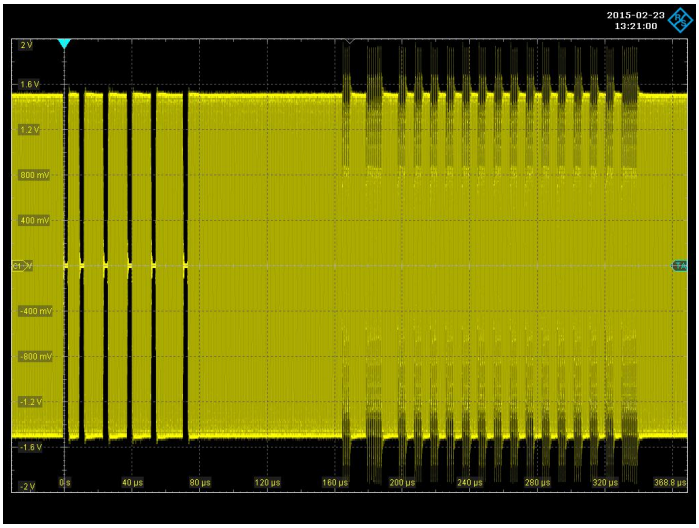

Fig. 3. Reader-to-Tag-link (left) and Tag-to-Reader-link (right)

More power leads to a decrease of the modulation index and signal to noise ratio (SNR), resulting in a smaller effect on the activation antenna. Therefore we started working with two antennas, one for activating the tag, one for receiving its response. This separation is possible because the information from the reader and tag is not only present in the fundamental frequency band (13.56 MHz ± 847.5 kHz) but also in multitudes of those frequency bands (2 x 13.56 MHz, 3 x 13.56 MHz, 4 x 13.56 MHz, 5 x 13.56 MHz, etc). The sidebands ($f_{harmonic}$± 847.5 kHz) contain the information of the tag.

There are different sources where the multitudes of the fundamental frequency could originate from: the tag, the reader, but also from the saturation of an amplifier. The most likely candidate to produce these frequency components is a non-linear component like the rectifying bridge in the tag, formed by four diodes D1 to D4 as shown in Fig. 4). These diodes load the antenna coil, modelled by L1, and provide a DC voltage for the rest of the circuitry of the tag.

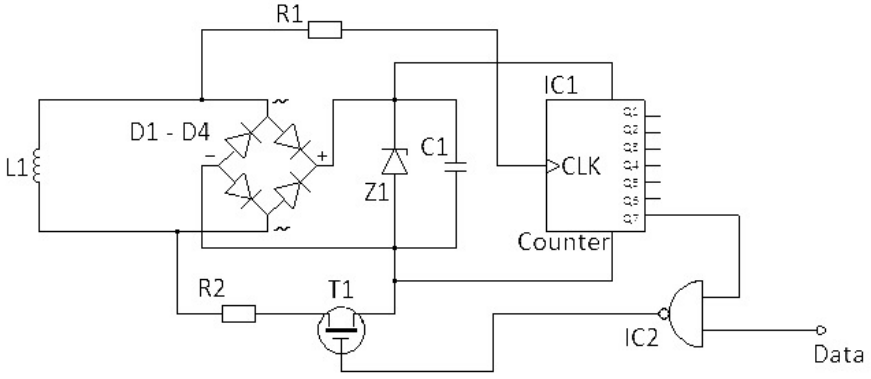

Fig. 4. Electrical circuit of a tag (adapted from: http://rfid-handbook.de/about-rfid.html)

To prove our conjecture that the higher harmonic signals originate from the tag, a self-made replica of a standard ISO/IEC 14443 tag was produced with the same dimension and characteristics as a standard RFID card. A comparison was made between two situations; without the diodes on the replica (Fig. 5) and with diodes mounted on the replica (Fig. 6).

The markers indicate the fundamental, 3$^{\text{rd}}$, and 5$^{\text{th}}$ harmonics. Measurements show that by mounting the diodes the power of all the harmonics increases and the power of the fundamental decreases. There is an increase with 15.43 dB for the 3$^{\text{th}}$ harmonic and with 29.3 dB for the 5$^{\text{th}}$ harmonic. At the same time the loading of the EM-field results in a decrease of the fundamental frequency of 6.17 dB. An overview of all the harmonics is shown in Table 1.

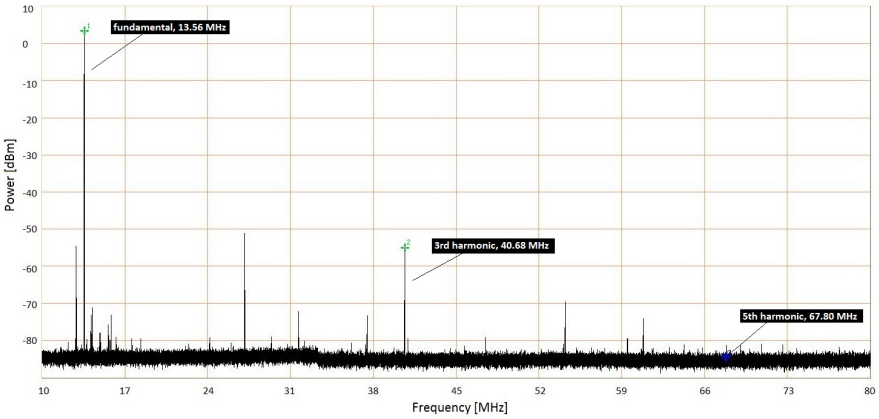

Fig. 5. Without diodes

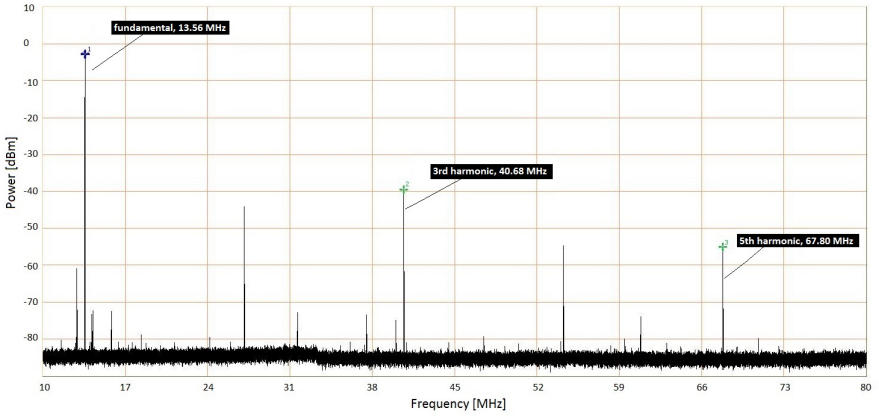

Fig. 6. With diodes

	1^{st} 13.56 MHz [dBm]	2^{nd} 27.12 MHz [dBm]	3^{rd} 40.68 MHz [dBm]	4^{th} 54.24 MHz [dBm]	5^{th} 67.80 MHz [dBm]
With diodes	7	-34	-30	-45	-45
Without diodes	13	-41	-45	-60	-74

Table 1. Higher order harmonics

These harmonics do not yet contain any information from the tag. They have to be modulated with the data from the tag (via IC2 and switch T1 in Fig. 4) before the information will be present in the frequency bands $f_{harmonic} \pm 847.5$ kHz.

A positive side effect when measuring the signal from the tag at these higher frequencies is that there will be less noise from the environment according to [3]. To measure the harmonics (and the modulation products) up to the 5^{th} order (67.80 MHz), a sensitive broadband antenna from the Lofar project[4] was available, that is normally used for astronomical observations. With the activation antenna from Section 3 it was possible to activate the tag at any distance up to 60 cm. The signal coming from the Lofar antenna was digitized with the National Instruments PXIe-5665 spectrum analyzer. In a LabVIEW program the results were digitally filtered and the spectra were extracted from the IQ data stream.

4.2 Results

With this set-up an eavesdropping distance of 3.7 meters was reached at which the answer of the tag (and the request from the reader) could still be retrieved. This distance can be reached measuring at 40.68 MHz (3^{rd} harmonic) and also at 67.80 MHz (5^{th} harmonic). In Fig. 7 the IQ data stream is shown measured with the National Instruments PXIe-5665 spectrum analyzer tuned to 40.68 MHz. The first peaks (until $\pm$ 80 μs) show data from the reader to the tag (REQA, REQuest command, type A [8]). The answer from the tag starts at $\pm$ 160 μs (ATQA, Answer To reQuest, type A). Comparing Fig. 7 with Fig. 3 it is clear that it follows the outline and time base of the AM-signal.

Engelhardt et al. already used higher harmonics for eavesdropping, reporting an eavesdropping range of 18 m, also using the 3^{rd} harmonic of the original signal [2]. They showed that cables attached to the reader were responsible for (re)transmitting the harmonics into free space and that with proper shielding of the reader these harmonics were undetectable. The same phenomenon occurs in our configuration and also [11] reports a high range for the Tag-to-Reader-link due to coupling effects.

Unfortunately, harmonics were only detected by the Lofar antenna if the tag was held in the corner of the activation antenna. Engelhardt et al. report the

[4] http://www.lofar.org

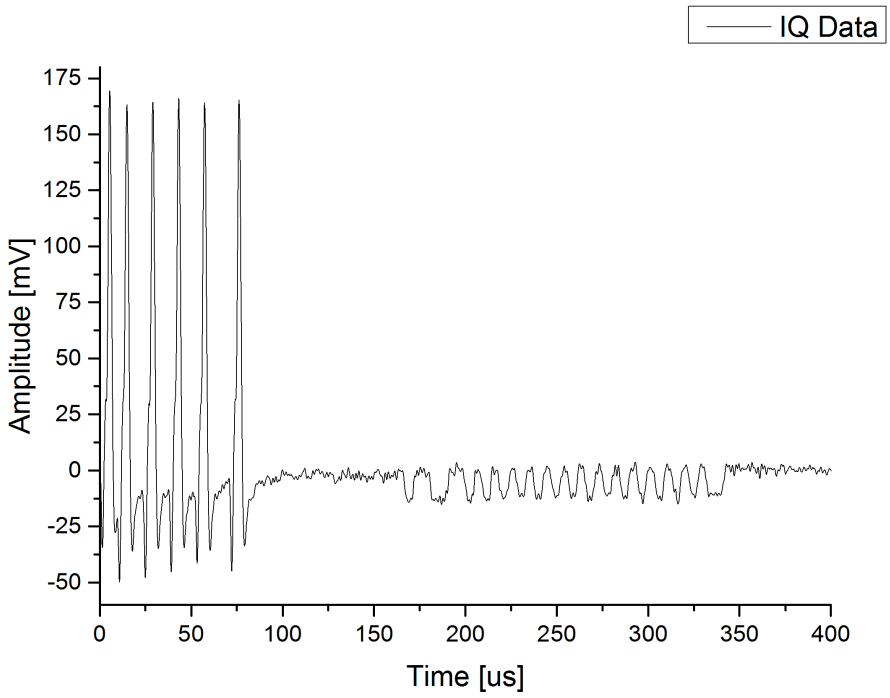

Fig. 7. Response at 40.68 MHz

same effect with the commercial RFID reader they used for activating the tag. They also had to place the tag in the corner of the reader to optimize results.

The observations made in the two paragraphs above, namely that (i) the modulated harmonics cannot be detected in the far field without a coupling effect to neighboring cables, and (ii) these higher harmonics are only present if the tag is held at a very precise location close to the reader, suggest that while the use of higher harmonics may be useful for passive eavesdropping attacks, it is not useful for active skimming attacks. After all, in a skimming attack the tag must be activated at a large distance. Concluding, the achieved eavesdropping distance looks promising but this set-up cannot be used in a skimming attack scenario.

5 Skimming using higher harmonics

5.1 Objective and test set-up

The RFID signal originates from the chip inside the reader as a square wave and contains all the harmonics according to the Fourier series. Together with

the fundamental frequency these harmonics are amplified, reach the activation antenna and, despite the fact that it is not tuned for these frequencies, they are still transmitted (mainly in the reactive near field). Besides the carrier, the tag modulates these harmonics resulting in a combined effect with the harmonics generated by the diodes on the tag (Section 4.1). Placed in the far field, the Lofar antenna could only receive the answer of the tag if this signal coupled into a nearby cable. It was not possible to place the Lofar antenna closer to the tag and activation antenna (in the near field) because it was too sensitive for the fundamental frequency. Although this fundamental frequency was outside the bandwidth of the antenna, the high power in the 13.56 MHz band still saturated the Lofar antenna and made a sensitive measurement impossible.

Measurements with a small pick-up coil in the near field of the tag showed that higher harmonics were still detectable at activation distances up to 20 cm. Besides that, we observed the decrease of power of the fundamental in the pick-up coil when placing the rectifying diodes in the self-made replica. This led to the idea of amplifying the third harmonic in the antenna of the tag by placing a second resonant coil in its near-field ($<$ 3.5 m) and use it as a receiving antenna. To prove this idea a new magnetic loop receiving antenna was made resonant at 40.68 MHz (undamped, resulting in a high Q-factor). Measurements with the receiving antenna placed at 12 cm from the tag showed an increase of the third harmonic of approximately 22 dB.

5.2 Results

Receiving the tag's response at a different frequency than the activation frequency makes it easier to retrieve the answer of the tag in the received signal. With the high power activation antenna and the selective receive antenna it is possible to use the maximum power available to activate the tag over a long distance, without the risk of damaging the receiving back-end and measurement equipment. With these two different antennas, tuned to two different frequencies, we made an RFID skimmer gate, shown in Fig. 8.

The square activation antenna, on the left side in the photo, is tuned to 13.56 MHz and activates the tag. The round receiving antenna, on the right side in the photo, is tuned to 40.68 MHz, enhances the 3$^{\text{rd}}$ harmonic and receives the reply of tag. It was also possible to tune the receive antenna to the 5$^{\text{th}}$ harmonic, but this did not result in a better reception of the answer. Albeit attenuated strongly, the carrier frequency is also received by the receiving antenna and, in contrast to the other antenna designs, without saturating the low-noise amplifier or reception circuit of the reader. The answer of the tag is decoded real time without any significant latency or delay.

The two main parameters in the configuration of our RFID gate are the width of the gate, i.e. the distance between the two antennas, and the activation power, i.e. the power from the amplifiers to the activation antenna. Each combination of width and power level results in a different communication range over which a tag can be activated and its response can be picked up. This communication range is determined at one end by the maximum activation distance and at the

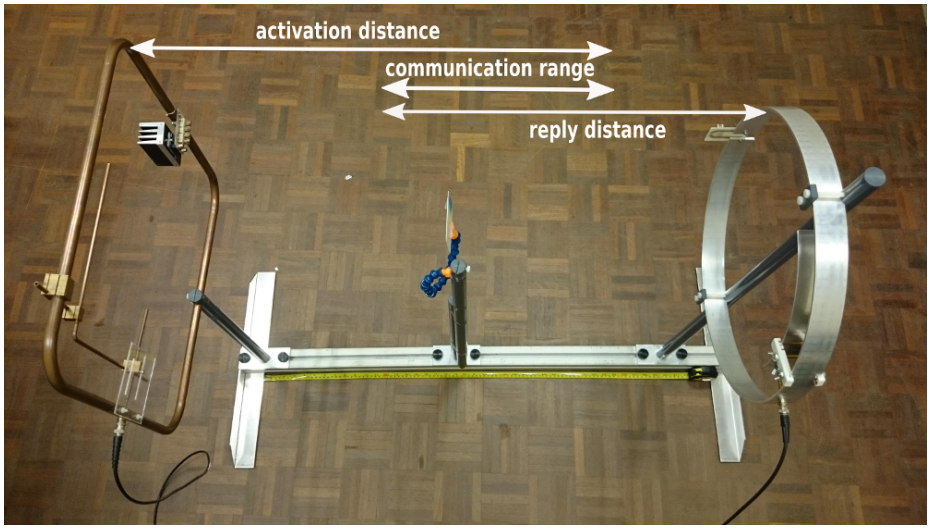

Fig. 8. RFID Skimming gate

Gate width [cm]	Power [W]	Activation distance [cm]	Reply distance [cm]	Communication range [from activation side of gate]
70	14-22	60	60	from 10 to 60 cm
90	14-22	75	20	from 70 to 75 cm
100	75-88	52.5	52.5	from 49.5 to 52.5 cm

Table 2. Results for RFID gate, where communication range is measured from the side of the gate formed by the activation antenna, i.e. the left side of the gate in Fig. 8

other end by the maximum reply distance. Table 2 gives the results achieved for three different widths of the gate, using different power levels:

- *An RFID gate of 70 cm.* Communication with a tag is possible over a range of 50 cm between the antennas, i.e. almost the full width of the gate except very close to either end. This is a major improvement compared to the earlier reported skimming distance of 25 cm [2].
- *An RFID gate of 90 cm.* This set-up achieves a long activation distance (of 75 cm from the activation antenna), while keeping the possibility to communicate with the tag at 20 cm of the receiving antenna. This is a substantial improvement of the maximum activation distances reported in the literature so far (27 cm) [3]. However, skimming – i.e. activating the card *and* receiving its response – is only possible over a very small range, 5 cm wide, in this configuration.
- *An RFID gate of 100 cm.* This configuration requires a large amount of power, and allows both activation and reception at just over 50 cm. It reaches

the maximum skimming distance: interaction with the tag is possible if it is held close to the middle of the gate.

The results above are obtained without the use of additional DSP software (Digital Signal Processing), using hardware from a standard card reader. We have strong indications that with better filtering techniques and a different amplifier longer distances and communication ranges are possible. The experiments were carried out using a standard ISO/IEC 14443A tag, where we used the reception of the card's UID upon activation as evidence that the card was working.

We also experimented with various types of cards to confirm that after sending their UID they can also carry out their normal functionality. They generally did, except that, as expected, the range may be reduced if this functionality requires a lot of computing power, esp. for asymmetric cryptography. For example, experiments using a programmable Java Card showed that, when using the same amount of activation power, the range over which the RFID gate can power an RSA computation on the card is smaller than the range over which it can power a DES or AES encryption. When gradually sliding the tag away from the activation antenna first RSA fails, followed by both DES and AES, which fail together with all functionality of the card. So for this card only RSA, and not AES and DES, required a shorter distance. Of course, such characteristics will be highly depend on the specific processor hardware inside a card.

We also observed the effect of the orientation of the tag by changing the position relative to the antennas. Ideally the tag is parallel with the antennas, for optimal inductive coupling. However, placing a tag at an angle of 45° with respect to the antennas still resulted in successful communication. Increasing the angle above 50° communication quickly deteriorated because of the reduced coupling.

Depending on the skimming scenario (secretly activate a tag and start a communication session) it is possible to tune the antenna arrangement. The most practical scenario will be the 70 cm gate. With this set-up a large communication range within the gate is achieved and not much power is needed (22 W compared to 88 W in the 100 cm set-up). The 70 cm gate width is wide enough to let people pass, and when the victim is forced to make a turn between the antennas (for example in a voting booth or fitting room), the chance of a successful readout is significantly increased. More compact solutions are also possible by placing the antennas close together (see Fig. 9). Here the tag does not have to be between the two antennas, but it can be held near them. Because the antennas are tuned to different frequencies there is little influence on each other and a skimming distance of 60 cm is achieved.

Currently, no commercial RFID readers are found achieving similar results for the ISO/IEC 14443A protocol. There are manufacturers that also use dual frequency technologies, but this requires non-standard tags equipped with two antennas. The advantage of the method presented in this paper is that widely available tags can be used without any adaption on the side of the tag and at the data rates the protocol specifies.

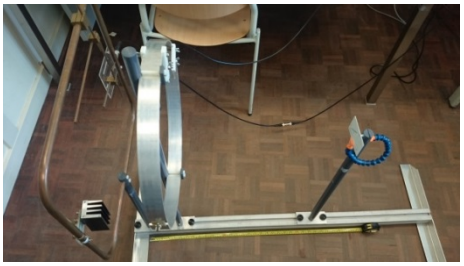

Fig. 9. Compact RFID Skimmer

6 Conclusions

We presented several antenna set-ups to study the practical communication limits of ISO/IEC 14443 Type A RFID technology. The final result is a new antenna design that significantly increases the communication range of RFID tags. The set-up is an RFID gate formed by two antennas, one activating the card at 13.56 MHz and another antenna receiving its response at the third harmonic frequency at 40.68 MHz. This RFID skimming gate is the first working prototype using higher harmonics for communicating with a tag over a long range in the near field.

The activation antenna can withstand 100 W, enough to activate the tag over a large distance. Normally when activating a tag over larger distances its answer cannot be received anymore due to the reduced coupling with the activation antenna. This is solved by enhancing and receiving the third harmonic of the tag's answer by placing a undamped loop antenna in the near field.

The two antennas can be placed in several configurations, for example to form

- a gate with a width of 100 cm, which can communicate with a tag held near the center between the two antennas, or
- a gate with a width of 70 cm, which can communicate with a tag over almost the entire range between the antennas.

Our results so far have been obtained without using any additional DSP (Digital Signal Processing) software. We have strong indications that with better filtering techniques and a different low-noise amplifier longer distances and wider communication ranges are possible.

References

1. The ARRL Antenna Book. The American Radio Relay League (2000)
2. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., Biebl, E.: Extending ISO/IEC 14443 Type A eavesdropping range using higher harmonics. In: Proceedings of 2013 European Conference on Smart Objects, Systems and Technologies (SmartSysTech). pp. 1–8. IEEE (2013)

3. European Radiocommunications Committee (ERC): ERC report 69 – propagation model and interference range calculation for inductive systems 10 kHz - 30 MHz (1999)
4. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. Wiley, 3 edn. (2010)
5. Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: Practical NFC peer-to-peer relay attack using mobile phones. In: Ors Yalcin, S. (ed.) Radio Frequency Identification: Security and Privacy Issues (RFIDSec 2010), LNCS, vol. 6370, pp. 35–49. Springer (2010)
6. Hancke, G.P.: Practical attacks on proximity identification systems. In: IEEE Symposium on Security and Privacy (S&P'06). pp. 328–333. IEEE (2006)
7. Hancke, G.P.: Practical eavesdropping and skimming attacks on high-frequency rfid tokens. J. Comput. Secur. 19(2), 259–288 (2011)
8. ISO/IEC: ISO/IEC 14443-3:2011, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision (2011)
9. Kfir, Z., Wool, A.: Picking virtual pockets using relay attacks on contactless smartcard. In: First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005). pp. 47–58. IEEE (2005)
10. Kirschenbaum, I., Wool, A.: How to build a low-cost, extended-range RFID skimmer. In: Proceedings of the 15th USENIX Security Symposium. pp. 43–57. Usenix (2006)
11. Oren, Y., Schirman, D., Wool, A.: Range extension attacks on contactless smart cards. In: Crampton, J., Jajodia, S., Mayes, K. (eds.) Computer Security – ESORICS 2013, LNCS, vol. 8134, pp. 646–663. Springer (2013)
12. Texas Instruments: HF antenna cookbook - technical application report 11-08-26-001 (March 2001)